AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

Eastern District of Virginia

United States of America
v.

OLABANJI OLADOTUN EGBINOLA

Case No. 3:19MJ224

Defendant(s)

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of 9/26/2018 to 12/26/2018 in the county of City of Richmond in the Eastern District of Virginia, the defendant(s) violated:

Code Section	*Offense Description*
1) 18 U.S.C. § 1343	1) Wire Fraud;
2) 18 U.S.C. § 1349	2) Conspirary to Commit Wire Fraud;
3) 18 U.S.C. § 1956(a)(1)	3) Money Laundering;
4) 18 U.S.C. § 1956(h)	4) Conspiracy to Commit Money Laundering.

This criminal complaint is based on these facts:

See attached Affidavit

☑ Continued on the attached sheet.

Complainant's signature

Stuart T. Voncanon, FBI Task Force Officer

Printed name and title

Sworn to before me and signed in my presence.

Date: 12/19/2019

/s/

Judge's signature

City and state: Richmond, Virginia

Roderick C. Young, United States Magistrate Judge

Printed name and title

AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT

I, Stuart T. VonCanon, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a task force officer (TFO) with the Federal Bureau of Investigation (FBI) and have been so employed since January 1, 2015. As such, I am charged with the duty of investigating violations of the laws of the United States as stated in Title 28 of the Federal Code of Regulations. I have extensive experience investigating various types of computer crimes, including criminal and national security computer intrusions, Internet fraud schemes, intellectual property rights violations, and theft of trade secrets. I have achieved Global Information Assurance Certifications as a Certified Incident Handler and Certified Forensic Examiner, and also in Information Security Fundamentals and Certified Security Essentials. I have received additional training through the FBI and various private sector entities in investigative techniques of computer crimes and advanced digital forensics. I have been involved in the investigation of matters concerning criminal intrusions of computer systems by foreign and domestic actors and also criminal violations relating to computer enabled fraud designed to induce victims to wire money to criminally controlled bank accounts. I have personally participated in the investigation described below.

2. I make this affidavit in support of a criminal complaint charging the following individual, OLABANJI OLADOTUN EGBINOLA (hereinafter "EGBINOLA"), with wire fraud, in violation of 18 U.S.C. § 1343, conspiracy to commit wire fraud, in violation of 18 U.S.C. § 1349, money laundering, in violation of 18 U.S.C. § 1956(a)(1), and conspiracy to commit money laundering, in violation of 18 U.S.C. § 1956(h).

3. This affidavit is being submitted for the limited purpose to show merely that there is sufficient probable cause for the requested arrest warrants and does not set forth all of my knowledge about this investigation. I have set forth facts that I believe are sufficient to charge EGBINOLA with the criminal conduct set forth herein.

RELEVANT STATUTORY PROVISIONS

4. **Wire Fraud:** 18 U.S.C. § 1343 makes it a crime when:

> Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice....

5. **Conspiracy to Commit Wire Fraud:** 18 U.S.C. § 1349 provides that any person who attempts or conspires to commit [wire fraud] shall be subject to the same penalties as those prescribed for the offense, the commission of which was the object of the attempt or conspiracy.

6. **Money Laundering:** 18 U.S.C. § 1956(a)(1) provides in pertinent part that whoever, knowing that the property involved in a financial transaction represents the proceeds of some form of unlawful activity, conducts or attempts to conduct such a financial transaction which in fact involves the proceeds of specified unlawful activity—

(A)(i) with the intent to promote the carrying on of specified unlawful activity; or

* * *

(B) knowing that the transaction is designed in whole or in part--

(i) to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity; or

(ii) to avoid a transaction reporting requirement under State or Federal law,

shall be sentenced to a fine of not more than $500,000 or twice the value of the property

involved in the transaction, whichever is greater, or imprisonment for not more than twenty years, or both. For purposes of this paragraph, a financial transaction shall be considered to be one involving the proceeds of "specified unlawful activity" if it is part of a set of parallel or dependent transactions, any one of which involves the proceeds of specified unlawful activity, and all of which are part of a single plan or arrangement.

7. **Conspiracy to Commit Money Laundering:** 18 U.S.C. § 1349 states that "[a]ny person who conspires to commit any offense defined in [] section [1956] or section 1957 shall be subject to the same penalties as those prescribed for the offense the commission of which was the object of the conspiracy."

8. **Specified Unlawful Activity:** The definition of "specified unlawful activity" is given in 18 U.S.C. § 1956(c)(7), which lists several categories of offenses that constitute "specified unlawful activity." Wire fraud, penalized under 18 U.S.C. § 1343, is included as a "specified unlawful activity" for purposes of money laundering in 18 U.S.C. § 1956(c)(7)(A), which in turn incorporates the list of "racketeering activities" set forth in 18 U.S.C. § 1961(1).

PROBABLE CAUSE

9. On or about September 26, 2018, an individual using the name "Rachel Moore" contacted an employee in the procurement department of a Virginia university using the email address accounts@kjellstromleegroup.com. The email address accounts@kjellstromleegroup.com is purposefully very similar to the actual email domain name for Kjellstrom and Lee, which is a large construction company located in Richmond, Virginia, and which has completed construction projects for multiple universities, including the same Virginia university. "Rachel Moore" advised the procurement department employee that the bank account on file for receiving payments was currently being audited and inquired if the next

payment could be sent to their foreign bank account. The university employee responded to "Rachel Moore" on September 28, 2018, with questions regarding the length of the audit and informed "Rachel Moore" that the university Treasury Department could assist her with setting up ACH transfers.

10. On October 4, 2018, "Rachel Moore" sent a reply email to the university employee stating:

> *Hope you are good. Thank you for the reply. In regards to the ACH setup, we can only have this done after the audit. The audit is usually between 4 and 6 weeks. Our CFO advised if we can have our payments sent by wire, and we setup the ACH once the audit is over. Will this be a possibility? Kindly get back to me as soon as you can. Thank you for your time.*

11. The university employee responded to "Rachel Moore" on the same day and told "Moore" to contact the university once the audit was complete to get assistance with setting up ACH wire transfers. They further advised "Moore" that a form is required to setup ACH transfers and it would need to be sent to the university Treasury Department as they are the ones who enter the account information into the payment system.

12. On October 24, 2018, "Rachel Moore" contacted the university and asked, "Hope you are good. Do you have any payment for us?" The university employee responded on October 25, 2018 by stating, "The last payment I am showing in our system, was issued on check 31499151, in the amount of $1,401,569.76. If you have any open invoices, please email them to me. Thank you!"

13. On October 30, 2018, "Rachel Moore" sent a message to the university employee stating:

> *Can you please confirm when check 31499151 was issued or sent out. In regards to the audit, we need to confirm what month to apply the payment to, in terms of when it was received. Thank you for your time.*

14. On the same day, the university employee responded with a screenshot from the payment processing system showing the details of the most recent transaction.

15. Later, on October 30, 2018, "Rachel Moore" sent a follow-up message to the university employee that stated:

> *Thank you for the information. We have not signed up to receive ACH payments yet, as we still have the audit ongoing, so please kindly notify us before our next payment is issued. Thank you for your time.*

16. The university employee responded to "Rachel Moore" and asked if there were currently any open orders with the university as there were currently no pending payments for their account.

17. On November 1, 2018, the university employee sent a follow up message to "Rachel Moore" stating, "There is a payment scheduled for today's check run. A check number has not been assigned as of yet, but the amount is $607,061.17. Reference number EP250XXXX."

18. On December 10, 2018, "Rachel Moore" sent the following message to the university employee:

> *Hope you are good. We signed up for ACH a couple of weeks ago, but a remittance email was not requested. Can you please notify us at remittance@kjellstromleegroup.com when a payment has been made. Can you please also confirm our last payment was on the 1st of November. Thank you.*

19. The university employee responded on December 11, 2018, and stated, "Check 3150XXXX was issued on 11-16-18, in the amount of $660,259.31. ACH was set up on 11/20/18; therefore, future payments will be sent directly to your account. Thank you!"

20. On December 20, 2018, the university initiated a payment via ACH wire transfer in the amount of $469,819.49 from their bank account to an account with the Bank of Hope, as listed in the ACH setup form provided by "Rachel Moore." On January 3, 2018, the university

was contacted by their bank, which was concerned the December 20, 2018 wire transfer was fraudulent. The university contacted Kjellstrom and Lee and learned they did not have an employee named "Rachel Moore" and that no establishment of ACH wiring had been initiated by Kjellstrom and Lee.

21. The majority of the above-described $469,819.49 wire transfer could not be recovered and was a loss for the Virginia university. A trace of the proceeds of the $469,819.49 wire transfer revealed that after the money was deposited in the Bank of Hope account it was quickly redistributed to multiple different banks through at least fifty different wire and check transactions over the period from December 21 to December 26, 2018.

22. The FBI determined that the fraudulent domain "kjellstromleegroup.com," which is associated with the "accounts@kjellstromleegroup.com" email address used to defraud the Virginia university, was registered by someone using the account name "bridgetclark" through the Internet domain registrar NameCheap, Inc. ("NameCheap"). In addition to registering the "kjellstromleegroup.com" domain for "bridgetclark," NameCheap also provided email-hosting services for that account. In response to legal process, NameCheap provided records to the FBI revealing that "bridgetclark" registered more than 50 domains with names that are deceptively similar to the Internet domain names associated with legitimate construction companies. I know from my training and experience that such deceptive domain names and associated email services are an integral part of many business email compromise schemes.

23. Records obtained from NameCheap strongly indicate that the individual(s) using the "bridgetclark" account employed a variety of techniques to conceal their true identity. The account was paid for using Bitcoin cryptocurrency, which can be difficult to trace because

Bitcoin "wallets" are accessible over the Internet using a variety of anonymizing techniques, including the Tor network.

24. Investigators reviewed IP log files provided by NameCheap for the "bridgetclark" account and determined that there was evidence of obfuscation there as well. Many of the IP addresses resolved to US-based networking providers including QuadraNet, Linode, and US Dedicated. All of these providers rent virtual private servers (VPS), provide virtual private network (VPN) services, and resell their IP address space to other providers who in turn provide VPN services, the upshot of which is that accessing the "bridgetclark" account through a VPN or VPS would conceal the user's true IP address. A number of other IP logons resolved to British telecomm companies. Cellular providers often provide mobile phone customers access to the Internet using a technology called network address translation, also known as "NATing," which assigns a single IP address to numerous cell phone numbers at the same time. Determining which cell phone user was responsible for a particular communication over the network of a cellular provider using NATing technology is a challenging, and sometimes impossible, task. Complicating matters further, cellular providers often maintain logs for only short periods of time, making it difficult to obtain the assistance of foreign law enforcement in time to contact the carrier and obtain identifying subscriber records.

25. On February 12, 2019, this Court also issued a search warrant pursuant to Rule 41(b)(6)(A), case number 3:19-sw-51, granting authority to the FBI to deploy a network investigative technique (NIT) to the email address accounts@kjellstromleegroup.com. On February 15, 2019, the individual accessing the email account accounts@kjellstromleegroup.com opened the email message containing the NIT and the code contained in the attached file executed, providing a variety of data to an FBI-controlled server, which included the IP address

of the computer opening the attachment. The IP address of the computer was 86.191.189.88, which is owned by British Telecom ("BT") in the United Kingdom.

26. In response to requests for assistance from the FBI, law enforcement officials in the United Kingdom provided information that on February 15, 2019, at the time the NIT was executed, IP address 86.191.189.88 was assigned to the subscriber Samiat Egbinola, address 56, Francisco Close, Chafford Hundred, Essex, RM16 6YD, with BT customer ID of BBEU16104626. Also identified as residing at the residence was the defendant, OLABANJI OLADOTUN EGBINOLA.

27. EGBINOLA was previously arrested in the United Kingdom in 2008 for money laundering. At the time of his arrest, a large quantity of US currency was seized from his residence. He was also in possession of a computer that contained information related to dozens of bank accounts of individuals who were victims of fraud. A review of EGBINOLA's bank account showed there was an expected annual income of £65,000 per year but there were no regular sources of income identified. The account was predominately funded by cash deposits that were quickly dispersed, which is indicative of a money laundering technique known as layering.

28. A review of US government records showed that EGBINOLA traveled to the US in 2016, at which time he provided to customs authorities a personal email address of aegbinola@gmail.com. EGBINOLA previously traveled to Los Angeles, California, in April 2015 and provided a destination address in Los Angeles that is associated with the subject of an FBI investigation for fraud and money laundering for schemes similar to the one being investigated by your affiant. EGBINOLA also traveled to Los Angeles, California, again in July

2019 and provided a destination address of a Los Angeles-based hotel that is approximately two miles from the address he visited in 2015.

29. According to records obtained from Google, the email account aegbinola@gmail.com was registered on May 16, 2008, from a BT IP address located in the United Kingdom. A review of the email headers contained in the aegbinola@gmail.com account showed numerous communications with multiple individuals, including with the email address xxxxxxxxxxxxx@yahoo.co.uk. This email address is associated with subject of another FBI investigation, who is a named defendant in a sealed indictment in the Western District of North Carolina relating to a similar fraud scheme targeting victims using spoofed domains of construction companies. Specifically, the xxxxxxxxxxxxx@yahoo.co.uk was used to receive invoices for VPN ("virtual private network") services that the fraudsters used to hide their true IP address information while committing the fraud scheme. Additionally, the same Yahoo account was used to receive information about construction companies that was later used to create spoofed domain names that were intrinsic to the fraud scheme. Messages between aegbinola@gmail.com and xxxxxxxxxxxxx@yahoo.co.uk were exchanged multiple times over a period of several years. The defendant under indictment in the Western District of North Carolina is associated with a company named Florian London, which is based in the UK. EGBINOLA listed Florian London as his employer on his travel documents when entering the United States in July 2019.

CONCLUSION

30. Based on the information detailed above, I respectfully submit there is probable cause to charge OLABANJI OLADOTUN EGBINOLA with the federal offenses of wire fraud,

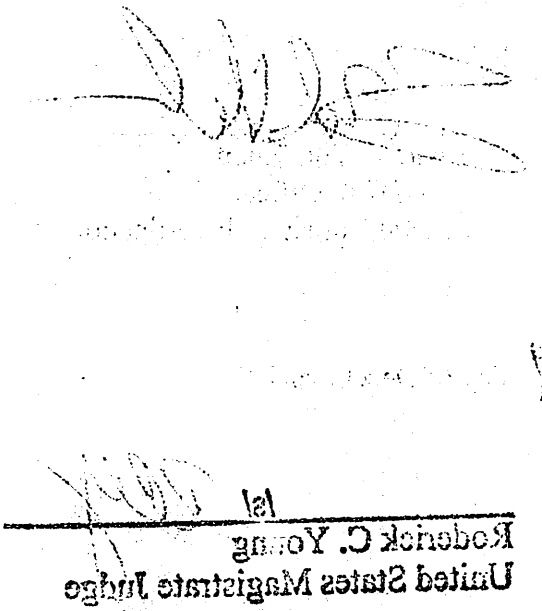
conspiracy to commit wire fraud, money laundering and conspiracy to commit money laundering.

Respectfully Submitted,

Stuart T. VonCanon
Task Force Officer
Federal Bureau of Investigation

SUBSCRIBED and SWORN before me this 19 day of December 2019.

/s/
Roderick C. Young
United States Magistrate Judge



/s/
Rodenick C. Young
United States Magistrate Judge